AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A cryptographic component, comprising:

a communication component that receives a request for decryption information from a BIOS component during an operating system boot process occurring after a hibernate mode; and,

a retrieval component that retrieves decryption information based, at least in part, upon the request, the retrieval component providing the decryption information to the communication component, the communication component providing the decryption information to the BIOS component during the operating system boot process occurring after a hibernate mode.

2. (Original) The component of claim 1, the decryption information comprising at least one of a decryption key, an encrypted decryption key and a decryption algorithm.

3. (Original) The component of claim 1, further comprising a storage component that facilitates storage of encryption information.

4-5. (Cancelled)

6. (Original) The component of claim 1 employed to secure access to at least one device.

7. (Original) The component of claim 6, the device comprising a storage volume, a video display, an input device and an output device.

8. (Currently Amended) A BIOS cryptographic system, comprising:

a BIOS component that facilitates a secure boot process of a computer system;

an operating system loader that facilitates loading of an operating system for the computer system; and,

a cryptographic component that serves as an interface between the BIOS component and the operating system loader, the cryptographic component providing decryption information to the BIOS component in response to a request for decryption information from the BIOS component to facilitate decryption of a file associated with a hibernate mode during an operating system boot process occurring after the hibernate mode.

9. (Cancelled)

10. (Original) The system of claim 8, the BIOS component employing a decryption algorithm to facilitate the secure boot of the computer system.

11. (Previously Presented) The system of claim 10, the decryption algorithm comprising a symmetric algorithm.

12. (Original) The system of claim 11, the decryption algorithm comprising RC2, RC4, Data Encryption Standard (DES), 3DES or AES.

13. (Original) The system of claim 10, the decryption algorithm comprising an asymmetric algorithm.

14. (Original) The system of claim 13, the decryption algorithm comprising RSA.

15. (Original) The system of claim 8, the decryption information comprising at least one of a decryption key, an encrypted decryption key and a decryption algorithm.

16. (Original) The system of claim 8, the cryptographic component comprising a decryption information store that securely stores the decryption information.

17. (Original) The system of claim 16, the decryption information comprising a decryption key.

18. (Original) The system of claim 17, the decryption key retrieved through an ACPI control method.

19. (Original) The system of claim 17, the decryption key retrieved through a BIOS boot interface.

20. (Original) The system of claim 8, the cryptographic component comprising an encryption information store that securely stores encryption information.

21. (Original) The system of claim 20, the encryption information comprising an encryption key.

22. (Original) The system of claim 20, the encryption key stored through an ACPI control method.

23. (Original) The system of claim 21, the encryption key stored through a BIOS boot interface.

24. (Original) The system of claim 8, the request for decryption information being based, at least in part, upon receipt of a BIOS password.

25. (Currently Amended) A method of securely restarting a computer system, comprising:

verifying a credential of a user;

retrieving decryption information; and

employing the decryption information to decrypt a hibernate file during an operating system boot process occurring after a hibernate mode.

26. (Original) The method of claim 25, the credential comprising a password.

27. (Original) The method of claim 25, the decryption information comprising at least one of a decryption key, an encrypted decryption key and a decryption algorithm.

28. (Original) A computer readable medium having stored thereon computer executable instructions for carrying out the method of claim 25.

29. (Currently Amended) A method of securely using a computer system, comprising:

verifying a credential of a user;

retrieving decryption information employing a decryption algorithm comprising an asymmetric algorithm; and

employing the decryption information to securely access a device during an operating system boot process occurring after a hibernate mode.

30. (Original) The method of claim 29, the decryption information comprising at least one of a decryption key, an encrypted decryption key and a decryption algorithm.

31. (Original) The method claim 29, the device comprising at least one of a disk, a volatile memory, a CD ROM and a storage device.

32. (Currently Amended) A method of facilitating secure restarting of a computer system, comprising:

receiving a decryption information; ~~and~~

securely storing the decryption information, the decryption information to be employed by a BIOS component during the restarting of the computer system from a hibernate mode; and

employing the decryption information by a BIOS component during the restarting of the computer system from the hibernate mode.

33. (Currently Amended) A data packet transmitted between two or more computer components that facilitates secure restarting of a computer system, the data packet comprising:

decryption information to be employed by a BIOS component to facilitate decryption of a hibernate file during the restarting of the computer system from a hibernate mode, the decryption information comprising at least one of a decryption key, an encrypted decryption key and a decryption algorithm.

34. (Currently Amended) A computer readable medium storing computer executable components of a cryptographic component, comprising:

a communication component that receives a request for decryption information from a BIOS component; and

a retrieval component that retrieves decryption information from a hibernate file based, at least in part, upon the request, the retrieval component providing the decryption information to the communication component, the communication component providing the decryption information to the BIOS component during a restarting of a computer system from a hibernate mode.

35. (Currently Amended) A cryptographic component, comprising:

means for receiving a request for decryption information from a BIOS component;

means for retrieving decryption information employing a decryption algorithm comprising an asymmetric algorithm based, at least in part, upon the request; and

means for providing the decryption information to the BIOS component during a restarting of the computer system from a hibernate mode.